Acceptable Use Policy

This document formalizes the policy for employees and contractors ("users") of all agencies under the Executive Office for Administration and Finance on the use of **information technology resources**; ("Agency ITRs"), including computers, printers and other peripherals, programs, data, local and wide area networks, and the Internet. In addition to this policy, individual agencies may choose to issue additional policies governing the use of Agency ITRs. Use of Agency ITRs by any employee or contractor shall constitute acceptance of the terms of this policy and any such additional policies.

1. User Responsibilities

It is the responsibility of any person using Agency ITRs to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgement in interpreting this policy and in making decisions about the use of ITRs. Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate management. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment.

2. Acceptable Uses

The Executive Office for Administration and Finance firmly believes that ITRs empower users and make their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, employees and contractors are encouraged to use ITRs to the fullest extent in pursuit of their Agency's goals and objectives.

3. Unacceptable Uses of Agency ITRs

Unless such use is reasonably related to a user's job, it is unacceptable for any person to use Agency ITRs:

- in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal
- for any political purpose
- for any commercial purpose
- to send threatening or harassing messages, whether sexual or otherwise
- to access or share sexually explicit, obscene, or otherwise inappropriate materials
- to infringe any intellectual property rights
- to gain, or attempt to gain, unauthorized access to any computer or network
- for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs
- to intercept communications intended for other persons
- to misrepresent either the Agency or a person's role at the Agency
- to distribute chain letters
- to access online gambling sites or
- to libel or otherwise defame any person.

4. Data Confidentiality

In the course of performing their jobs, Agency employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs.

5. Copyright Protection

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgement when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

6. Computer Viruses

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. Finally, it is a good practice to scan floppy disks periodically to see if they have been infected.

7. Network Security

Most desktop computers are connected to a local area network, which links computers within the Agency and, through the wide area network, to most other computers in state government. As such, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their passwords with anyone else, and should promptly notify Agency MIS personnel if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a password-protected screen savers in operation. Finally, no user is allowed to access the Internet or other external networks via modem unless they have received specific permission from Agency MIS personnel.

8. E-mail

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (first.last@state.ma.us), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that all e-mails are written in a professional and courteous tone. Finally, although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

9. No Expectation of Privacy

Agency ITRs are the property of the Commonwealth of Massachusetts and are to be used in conformance with this policy. The Agency retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the Agency will exercise the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. Users should be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of Agency ITRs constitutes express consent for the Agency to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access.